

UNITED STATES DISTRICT COURT

FILED

for the
Eastern District of Missouri

SEP 23 2016

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of

INFORMATION ASSOCIATED WITH IKHOJA@GMAIL.COM }
AND DISCEROS.CHEN@GMAIL.COM }
THAT IS STORED: AT PREMISES CONTROLLED BY }
GOOGLE, INC. }

Case No. 4:16 MJ 7259 SPM

APPLICATION FOR A SEARCH WARRANT

I, Robert Polanco, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:INFORMATION ASSOCIATED WITH IKHOJA@GMAIL.COM AND DISCEROS.CHEN@GMAIL.COM
THAT IS STORED: AT PREMISES CONTROLLED BY GOOGLE, INC.located in the Northern District of California, there is now concealed

See Attachments A&B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. Section 1030(a)(2)(C)
18 U.S.C. Section 1832

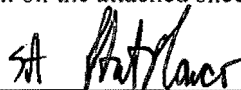
Offense Description

Fraud and Related Activity in connection with Computers
Theft of Trade Secrets

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

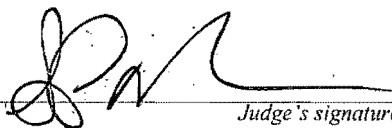


Applicant's signature

Special Agent Robert Polanco
Federal Bureau of Investigation

Printed name and title

Sworn to before me and signed in my presence.

Date: 9.23.2016City and state: St. Louis, MO

Judge's signature

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge

Printed name and title

AUSA: GWENDOLYN CARROLL

**IN THE MATTER OF THE SEARCH OF:
INFORMATION ASSOCIATED WITH
IKHOJA@GMAIL.COM AND
DISCEROS.CHEN@GMAIL.COM
THAT IS STORED: AT PREMISES
CONTROLLED BY GOOGLE, INC.**

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Robert Polanco, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with two certain accounts that are stored at premises controlled by Google, Inc., an email provider headquartered at 1600 Amphitheatre Parkway, Mountainview, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since March 2008. Since this time, I have taken a number of in-person and online training courses to enhance my understanding of counterintelligence investigative matters and a number of online training courses to enhance my understanding of cyber investigative matters.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 1030(a)(2)(C) (Fraud and Related Activity in Connection with Computers) and Section 1832 (Theft of Trade Secrets) have been committed by Jiunn Ren Chen. There is also probable cause to search the information described in Attachment A—specifically, target email addresses ikhoja@gmail.com and disceros.chen@gmail.com—for evidence, instrumentalities, contraband and fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States for the Eastern District of Missouri that has jurisdiction over the offense being investigated.

DEFINITIONS

6. The following terms may be used in the affidavit and are defined as follows:

- a. The term “computer,” as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as an “electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.”

- b. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- c. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- d. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- e. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not

limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

- f. “Computer passwords” and “data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- g. “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might be static whereby the user’s ISP assigns his computer a unique IP

address – and that same number is used by the user every time his computer accesses the Internet. Numerical IP addresses generally have corresponding domain names. For instance, the IP address 149.101.10.40 traces to the corresponding domain name “www.cybercrime.gov”. The Domain Name System or DNS is an Internet service that maps domain names. This mapping function is performed by DNS servers located throughout the Internet. In general, a registered domain name should resolve to a numerical IP address.

- h. “Internet addresses” take on several forms, including Internet Protocol (IP) addresses, Uniform Resource Locator (URL) addresses, and domain names. Internet addresses are unique and can be traced to an identifiable physical location and a computer connection. The Internet Protocol address (or simply “IP” address) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.187). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address, it enables Internet sites to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs. There are two types of IP addresses, dynamic and static. To assign dynamic IP addresses, the ISP randomly assigns one of the available IP addresses, in the range of IP addresses controlled by the ISP, each time a customer dials in or connects to the ISP in order to connect to the Internet. The customer’s computer retains that IP address for the duration of that session (i.e., until the user

disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, that IP address becomes available to other customers who dial in at a later time. Thus, an individual customer's dynamic IP address may, and almost always will, differ each time he dials into or connects to the ISP. To assign static IP addresses, the ISP assigns the customer a permanent IP address. The customer's computer would then be configured with this IP address every time he dials in or connects to the ISP in order to connect to the Internet.

- i. The "Internet" is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of sharing information. Connections between Internet computers exist across state and international borders and information sent between computers connected to the Internet frequently crosses state and international borders, even if those computers are in the same state. A network is a series of devices, including computers and telecommunication devices, connected by communication channels.
- j. An "internet service provider" (ISP) is a commercial service that provides Internet connectivity to its subscribers. In addition to providing access to the Internet via telephone lines or other telecommunications lines, ISPs may also provide Internet e-mail accounts and other services unique to each particular ISP such as Usenet Newsgroups and Internet Relay Chat. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account

application information, customer service information and other information, both in computer data format and in written record format.

- k. A “server” is a centralized computer that provides services for other computers connected to it via a network. The computers that use the server's services are sometimes called “clients.”
- l. Virtual Private Networks (hereinafter referred as “VPNs”) give extremely secure connections between private networks linked through the internet. Some of the advantages of using VPNs are it facilitates the accessing of a company’s computers from private residences as well as from anywhere in the world, provided that VPN client software is installed on the laptop.

BACKGROUND CONCERNING EMAIL

7. In my training and experience, I have learned that Google, Inc. provides a variety of online services, including electronic mail (“email”) access, to the public. Google, Inc. allows subscribers to obtain email accounts at the domain name gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google, Inc. During the registration process, Google, Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google, Inc. are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google, Inc. subscribers) and information concerning subscribers and their use of Google, Inc. services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

8. A Google, Inc. subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than those attached to emails), and

other files, on servers maintained and/or owned by Google, Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails in the account, and attachments to emails, including pictures and files.

9. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provides clues to their identity, location or illicit activities.

10. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

11. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

12. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into

an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

PROBABLE CAUSE

Summary

13. From 2010 to 2014, Jiunn Ren Chen (hereinafter referred to as "Chen") worked for Monsanto. Chen subsequently worked for The Climate Corporation (hereinafter referred to as "TCC") from 2014 to June 1, 2016. TCC is a subsidiary of Monsanto. In recent months, it has come to the attention of Monsanto, and the FBI, that after his resignation from Monsanto/TCC, Chen accessed a cloud storage device and copied 63 files containing trade secret information belonging to Monsanto and TCC. Further, during the course of the investigation, it was determined that Chen had also emailed some of Monsanto's trade secret information to his personal email account and his wife's personal email account in the calendar years 2014 and 2015. Based on FBI and Monsanto's investigative results, this Court issued a search warrant for Chen's residence that was executed by Special Agents and Forensic Examiners assigned to the FBI's St. Louis Division on June 16, 2016. FBI personnel subsequently analyzed forensic images of a computer and computer-related devices that were located in Chen's residence during the execution of this search warrant. Moreover, right before Chen's resignation from Monsanto/TCC, he traveled to China with his TCC MacBook laptop for a job interview with Sinochem China National Seed ("Sinochem"), a competitor of Monsanto, and was offered a job with Sinochem. Chen took the TCC MacBook Laptop with him to the job interview in China. The TCC MacBook

Laptop was provided to Chen by TCC and was capable of accessing TCC and Monsanto's cloud storage accounts that contained trade secrets. GPS records of the TCC MacBook laptop revealed that Chen returned to the United States from China on May 15, 2016. On August 20, 2016, Chen and his family flew to China after purchasing one-way airline tickets the night before. While in China, Chen has been corresponding using target email account disceros.chen@gmail.com. As detailed herein, there is probable cause to believe that Chen used his email account and his wife's email account to facilitate his theft of TCC's and Monsanto's trade secrets.

Employment History

14. From 2010 to 2014, Chen worked for Monsanto, a company that delivers agricultural products that support farmers all around the world. Specifically, Monsanto produces and develops agricultural and vegetable seeds, plant biotechnology traits and crop protection chemicals. While employed by Monsanto, Chen worked on many projects related to seeds and biotechnology traits. In 2014, Chen started working for TCC after it was acquired by Monsanto. Chen worked on data analytics and product concepts while with TCC. TCC combines hyper-local weather monitoring, agronomic modeling and high-resolution weather simulations to help farmers improve profitability by making better informed operating and financing decisions. Monsanto acquired TCC to serve as the foundation for Monsanto's vision of an agricultural "Google." Monsanto had such strong faith in TCC's potential viability that it paid approximately one billion USD for it. Monsanto estimates that TCC will be worth twenty-five billion USD in the future.

15. On June 1, 2016, Chen submitted his written two-week resignation to Monsanto/TCC. Chen's stated reason for resigning was that he wanted to move back to Taiwan to spend more time with

his family. Chen verbally claimed to co-workers that he wanted to be closer to his ill father, who works in the real estate business in Taiwan.

16. On June 2, 2016, Chen returned two laptop computers—that are owned by Monsanto and were issued to Chen for work purposes—to Monsanto: a MacBook Pro (“MacBook”), serial number C0ZMF4GJFD57, used by Chen when he worked for TCC; and a Lenovo ThinkPad T440 (“ThinkPad”), serial number PF0Z6XDR, used by Chen when he worked for Monsanto. TCC’s Information Technology (hereinafter referred to as “IT”) personnel assumed custody of these laptops, conducted a log check of software on the MacBook, and subsequently discovered suspicious software. Specifically, on June 2, 2016, TCC IT personnel gave the laptops to Monsanto’s Information Security Office forensic team (ISO). ISO performed an overall analysis of these laptops in accordance with Monsanto’s standard operating procedure when dealing with employee departures. This led to the discovery that the following software was contained on the MacBook: GNU Privacy Guard (GPG) encryption package, which allows the encryption and signing of data and communications and features a versatile key management system and access modules for all kinds of public key directories; a Secure Delete application, which overwrites data in a file to make the deleted data no longer accessible; and three Virtual Private Networks (VPNs), which create encrypted connections over less secure networks. Monsanto ISO personnel advised that, together, these software packages would effectively mask any nefarious cyber activity conducted on the MacBook. Monsanto ISO personnel also discovered that the Lenovo ThinkPad T440 had a number of network scanning tools, which, when used in combination, would allow an individual to covertly look within a network for vulnerabilities. These network scanning tools include Wireshark, which is a network protocol analyzer; Fiddler, which is used to troubleshoot and analyze networks; various torrents, which are used to distribute files over the internet; C Cleaner, which is used to scan computers for temporary files or private browser information and delete them it

from computers; and various malware, which is malicious software designed to damage or disrupt a system. Chen's supervisor advised that Chen did not have a legitimate reason for having any of this listed software on the MacBook Pro or the Lenovo ThinkPad T440 because it did not pertain to Chen's work responsibilities.

17. Based on information I received from Monsanto forensic experts and FBI forensic experts, as well as my training and experience, I know that these software packages can be used to locate, intrude on, obtain, procure, and copy files and data and then conceal the intrusion. Monsanto ISO personnel also advised the FBI that a mass data deletion took place on both laptops on June 1, 2016, the day of Chen's resignation. Members of the FBI St. Louis Division's Computer Analysis Response Team (hereinafter referred to as "CART") determined the mass deletions started at approximately 8:35 a.m. and finished at approximately 10:02 a.m. on June 1, 2016. A second mass deletion took place on the same day. This second mass deletion started at approximately 12:48 p.m. and finished at approximately 2:09 p.m. This resulted in Chen having a very small digital footprint of work product and personal files on either laptop.

Sequence of Events

18. On or about June 7, 2016, Monsanto personnel scheduled an interview with Chen to discuss the presence of the aforementioned software packages on the two laptops. The interview between Chen and Monsanto personnel took place on June 9, 2016, at the Starbucks coffee shop located at 6622 Chippewa Street, St. Louis, Missouri 63109. This location was selected by Chen. The interviewing team of Monsanto personnel asked Chen a number of questions related to the presence of the aforementioned software packages on the TCC MacBook Pro and Lenovo ThinkPad T440 laptops. Chen denied having any knowledge of the software packages' capabilities.

19. As the conversation progressed, Chen provided conflicting answers to questions. For instance, he told the Monsanto personnel he deleted everything on his laptops by placing everything in the trash bin and then “securely deleted it.” Chen later amended this statement and said he simply emptied the trash bin. Monsanto personnel asked Chen to explain this process. Chen responded by saying, “I didn’t download the program,” but later said, “I used the secure delete.” Chen stated that he used secure delete because he did not want anyone to view his personal files on the laptops, and he claimed that another employee had told him that Monsanto accesses employees’ personal files after they return their laptops.

20. Chen also claimed to have had “drop boxes”¹ for both laptops for data storage purposes. Chen further claimed to have hardly used the Lenovo ThinkPad T440 since 2013 for reasons other than to access Monsanto’s library, establish calendars and use his work email for personal communications pertaining to his divorce and a house purchase. These statements are inconsistent with Monsanto ISO personnel’s discovery that two USB drives had been inserted into the Lenovo ThinkPad since April 2016. Chen claimed he used the USB drives to copy and save photographs of his child. Moreover, Chen claimed that he had not accessed the Google Drive² account associated with the MacBook since June 1, 2016. Monsanto employees regularly work from home using their work-issued laptops and iPhones. They can access Monsanto’s networks from home through these devices.

21. On June 13, 2016, Monsanto ISO personnel discovered the unauthorized use of another TCC employee’s account on Chen’s TCC MacBook. The account belonged to “J.C.,” a customer

¹ “Drop boxes” are a type of cloud storage.

² Google Drive is an online file storage system that allows users to store their files in the cloud, share these files, and edit documents.

support employee, who does not work with IT support and is not part of Chen's working group. This use took place at approximately 7:25 a.m. on June 1, 2016, the day of Chen's resignation, but before Chen returned the MacBook to Monsanto on that same day. On June 13, 2016, Monsanto ISO personnel interviewed J.C. who stated that he did not know Chen, did not log onto Chen's MacBook, and did not know why his (J.C.'s) account would have been accessed via Chen's laptop.

22. Shortly thereafter, Monsanto personnel discovered that approximately 63 files were downloaded from Chen's TCC Google Drive account between June 1, 2016 and June 10, 2016. These downloads took place after Chen returned the TCC MacBook Pro and Monsanto Lenovo ThinkPad T440 laptops. Two passwords are required to access Chen's TCC Google Drive, and Chen still possessed both of these passwords between June 1, 2016 and June 10, 2016. Although Chen turned in his resignation, Monsanto did not specifically inform Chen he could not access Monsanto's network. Chen had access to these networks since he signed Monsanto's Employee Agreement on May 3, 2010. Monsanto's Employee Agreement explained Monsanto's confidential and non-compete policies as it pertains to Monsanto's intellectual property. These policies specifically state that an employee shall use their best efforts and diligence to protect Monsanto's confidential and trade secret information and shall not disclose any confidential or trade secret information both during and after employment with Monsanto (or Monsanto's subsidiary). Further the agreement includes a "Non-Compete" section which states that the employee cannot disclose confidential information so long as it shall remain proprietary or protectable as confidential or trade secret information of Monsanto (or Monsanto's subsidiary).

23. Monsanto's Business Conduct Office and TCC leadership stated that all 63 of these files contain confidential trade secrets and proprietary sensitive material. It is unknown at this time whether the files are individually password protected. What is known is the files are a mixture of strategies, analytical products, working notes and presentations regarding a number of Monsanto's projects. In

combination, they are of very high importance to Monsanto's overall economic viability as an organization and include pending projects, which Monsanto protects via a variety of methods. These methods include the granting of access to trade secret information to specific individuals with a need to know, the issuance of credentials that authorize these specific individuals to enter project labs where the research and development of Monsanto's trade secret information takes place, and the collaboration with Monsanto's Intellectual Property Counsel to evaluate the risk of releasing research project information via patents versus keeping the information a trade secret. This last measure is key because, while U.S. patents are valid for 20 years, foreign competitors are not restricted from replicating and producing Monsanto products because U.S. patent laws do not apply to them. Chen was allowed to access Monsanto's trade secrets while he worked for Monsanto/TCC due to his position with the company. Chen worked on TCC's data analytics and predictive analysis projects, which contained company trade secrets.

24. Monsanto advised TCC personnel were informed Chen had transferred all of his work responsibilities to other co-workers weeks prior to his resignation. Accordingly, there was no legitimate reason for Chen to access TCC's cloud storage or to download files from it. The following is a listing of all downloads from Chen's TCC Google Drive account spanning from June 1, 2016 to June 10, 2016. According to Chen, only he had access to his TCC Google Drive account, TCC MacBook Pro, and Monsanto Lenovo ThinkPad T440, and no one else had the passcodes to these accounts. Because the titles of these downloaded files are highly sensitive in nature, the titles are not listed in this affidavit but they are known to law enforcement.

- a. Username: jchen@climate.com
- b. Action: File Downloads
- c. Activity Dates:

- i. June 1, 2016, six downloads took place at approximately 7:36 p.m.
- ii. June 2, 2016, two downloads took place between 6:58 p.m. and 11:19 p.m.
- iii. June 4, 2016, one download took place at approximately 7:29 a.m.
- iv. June 5, 2016, one download took place at approximately 4:26 a.m.
- v. June 6, 2016, one download took place at approximately 8:37 p.m.
- vi. June 8, 2016, one download took place at approximately 3:32 p.m.
- vii. June 10, 2016, 51 downloads took place at approximately 3:47 a.m.

1. Given the sheer volume of these 51 downloads with a singular timestamp, Monsanto ISO personnel advised this could not have been downloaded via a cellular phone. Accordingly, the download would have had to occur on another computing device.

- d. Monsanto has not yet determined the location to which these files were downloaded.

25. Normal Monsanto business hours are between 7:00 a.m. and 5:00 p.m. Central Time.

The June 10, 2016 downloads occurred very early in the morning—before work hours—the day after Monsanto's interview of Chen.

26. On June 14, 2016, Monsanto employees again interviewed Chen, this time in the presence of a FBI Agent who did not reveal her affiliation with the FBI. Chen was asked about his iPhone, and he offered Monsanto the opportunity to examine the phone to look for any downloaded data. Chen admitted to deleting his Gmail account and certain applications prior to the interview because he thought that Monsanto would ask to examine his phone. Monsanto employees reviewed the phone and determined that his iPhone had been wiped clean. When asked about the 63 downloaded documents, Chen denied downloading the documents. Monsanto employees showed Chen the list of documents,

and Chen advised them that he was familiar with the documents and proceeded to describe them based only on the names of the documents. Although Chen did not describe this information as “trade secrets,” Chen acknowledged this information was confidential business information.

27. During Monsanto’s interview of Chen, Chen admitted to going on a job interview for Sinochem, which is currently involved in a joint venture with Monsanto. Dr. Jun Hua Peng, who is a former Monsanto employee who left Monsanto in 2014 to join Sinochem, interviewed Chen. The job interview took place in May 2016, in China. Chen stated he was offered a job with that company and was strongly considering the job offer. During the interview, Chen also stated that he did not have a computer in his residence, but his wife did. He further stated that his wife also had a hard drive and a USB drive. He additionally stated that his wife was an attorney and may have had legal files and client information on her computer. Chen then showed Monsanto personnel a hard drive that he had brought with him to the interview. Chen stated the hard drive belonged to his wife, with whom he resided. Chen would not allow Monsanto to look at the hard drive.

28. Chen has acknowledged that: (1) he used thumb drives; (2) his wife had a computer in their residence; and (3) he had a strong familiarity with cloud-based computing. Monsanto officials have stated that Chen “worked and lived in the cloud.”

Authorization to Search Chen’s Residence

29. On June 16, 2016, the United States District Court Magistrate Judge Noelle Collins authorized a search warrant for Chen’s residence. The search warrant was based on a violation of 18 U.S.C. § 1030(a)(2)(C) and authorized the search of Chen’s residence for evidence, contraband, fruits of this crime, and instrumentalities of this crime. On June 16, 2016, Special Agents and Forensic Examiners assigned to the FBI’s St. Louis Division (hereinafter referred as “St. Louis Division”) executed the search warrant. During the search, the Forensic Examiners made forensic copies of a

number of different electronic media in Chen's residence for future analysis. Additionally, Special Agents interviewed both Chen and Irma Khoja (hereinafter referred to as "Khoja"), who is Chen's current wife.

30. During the FBI interview of Chen, Chen said he reached out to Jun Hua Peng, who worked for Sinochem prior to August 2015. Chen stated that he and Peng spoke over the telephone. During his conversation with Peng, Chen expressed interest in a job with Sinochem. Since the initial contact, Chen stated that he continued to have contact with Peng approximately every two to three weeks via We Chat (hereinafter referred to as "WC"), which is a social media digital application that facilitates the exchange of information between numerous individuals. Chen claimed he and Peng exchanged online articles via WC. Chen continued on to state that in March 2016, Peng offered Chen a job. Chen stated he traveled to China for approximately one week in early May 2016 for a job interview associated with Peng's offer.

31. While in China, Chen stated he met with representatives of the Life Sciences Center (hereinafter "LSC"). These individuals were Peng, Qi Fa Zhang and Fa Song Zhou. Zhang was the director and figurehead of the LSC, as well as a member of the American National Academy of Sciences. Zhou, who Chen said previously worked for Monsanto approximately six years ago, was the director of molecular breeding at LSC. Monsanto has no record of Zhou's former employment with Monsanto and does not know whether Zhou ever worked for TCC. Chen advised that at some point during the trip, Peng pointed to a specific position on LSC's organizational chart and told Chen that the position of Director of Resource Management and Bio-informatics was Chen's, if Chen chose to accept the position. At the time of the offer, Chen explained that Peng served in two capacities at the LSC, as Vice Director and as the Director of Resource Management and Bio-informatics. Chen told this affiant that he planned to move to China in approximately three to four months if he accepted Peng's offer,

which would be for less monetary and compensation benefits than Chen earned while working for Monsanto. Additionally, Chen said he would work in Wuhan, China, which is approximately two hours away by plane from his father's home in Taipei, Taiwan. Chen stated that no one asked him about his Monsanto-related work while in China.

32. During the FBI interview of Khoja, Khoja advised Chen contacted China National Seed, which Chen previously advised is owned by Sinochem, for a job interview in December 2015. Khoja stated that in May 2016, Chen and Khoja spent approximately 10 days in China and a couple of days in Taiwan visiting family. While in China, Khoja stated Chen met with a man whose last name was Peng for a job interview with China National Seed. Per Khoja, Chen took his TCC MacBook and passport in a backpack to the job interview. Khoja stated that China National Seed offered Chen a job during this trip, but Chen did not accept it right away, and both Khoja and Chen were still discussing it. Per Khoja, Chen would earn less money there than at Monsanto. Khoja advised Chen attempted to install VPNs onto the TCC MacBook while in China because Chen and she wanted to use it for social media purposes. Chen attempted to download several VPNs, but the Astrill VPN did not work, so they ended up using the Express VPN instead.

Monsanto's and Speartip's Investigation

33. Following the execution of the aforementioned search warrant for Chen's residence, Monsanto directly advised the FBI that Chen, without authorization and against company policy, emailed some of its from his TCC email account to the target email accounts, specifically, Khoja's ikhoja@gmail.com personal email account and Chen's diceros.chen@gmail.com personal email account. Monsanto confirmed these transactions after Chen admitted through his attorney to having done so. Monsanto subsequently focused its internal investigative efforts on Chen's email traffic and

discovered Chen emailed the trade secret information from his TCC email on the following dates and times:

- a. Tuesday, August 19, 2014 at 4:11 p.m. to ikhoja@gmail.com
- b. Wednesday, November 5, 2014 at 2:16 p.m. to dicerros.chen@gmail.com
- c. Wednesday, November 12, 2014 at 3:54 p.m. to ikhoja@gmail.com
- d. Saturday, February 14, 2015 at 5:36 p.m. to dicerros.chen@gmail.com
- e. Saturday, February 14, 2015 at 5:36 p.m. to dicerros.chen@gmail.com

34. Monsanto's Chief Scientist reviewed the aforementioned emails and confirmed they contained very rich trade secret information, which Monsanto attempted to protect via a three prong approach.

35. Monsanto, via its Husch Blackwell legal counsel (hereinafter referred to as "Husch Blackwell"), advised that Chen used jchen@climate.com, his TCC email account, to email approximately 37 document attachments³ to himself at jchen@climate.com between April 5, 2016 and April 6, 2016. Monsanto believes, but its Chief Scientist has not yet confirmed, that these attachments contained some of Monsanto's trade secret information. Monsanto, also via Husch Blackwell, advised that 15 of the 37 attachments were accessed on the Monsanto Lenovo ThinkPad laptop T440 computer. This happened prior to April 6, 2016. Monsanto's investigation has revealed that a Kingston brand thumb drive was inserted into the Monsanto Lenovo ThinkPad laptop on April 6, 2016.

36. The St. Louis Division of the FBI reviewed the aforementioned emails that Chen sent himself with document attachments. The FBI counted the emails and attached documents and discovered that out of a total of 29 emails, there were 39 attached documents that Chen sent himself.

³ The document attachments on the email included power point presentations, word documents, and pdf documents.

Additionally, the FBI discovered via a comparison and review of Speartip's initial/preliminary forensic analysis results, that 12 of the document attachments were accessed on Monsanto's ThinkPad Lenovo T440 prior to the insertion of the Kingston thumb drive. Of these 12, one was accessed on April 5, 2016, and 11 were accessed on April 6, 2016.

37. Speartip digital forensic analysts (hereinafter referred to as "Speartip"), were contracted by Monsanto in connection with its civil litigation efforts against Chen. Speartip has been reviewing computer forensic evidence in Monsanto's possession. Speartip advised the FBI that 51 files and folders were accessed on Monsanto's Lenovo ThinkPad laptop between April 5, 2016 and April 6, 2016. Of these 51 files and folders, seven files were printed on April 6, 2016 at approximately 1:22 p.m. within seconds of each other. This print job took place after the Kingston thumb-drive had been inserted to Monsanto's Lenovo ThinkPad laptop on April 6, 2016 at approximately 1:15 p.m.

38. Speartip advised that the aforementioned Kingston thumb-drive was also inserted into the TCC MacBook Pro laptop computer on or about May 12, 2016, while Chen was in China and/or Taiwan.

39. Speartip also advised that Chen's TCC Google Drive account was accessed via an anonymized IP address, which was identified as 104.238.32.44, on or about May 9, 2016 when Chen was in China. This is significant because it shows the TCC MacBook was used in China and Chen accessed a cloud storage account of TCC that contains trade secrets while in China. Further, Chen's claim to the FBI that he traveled to China without the TCC MacBook is refuted by the following information. Specifically, Khoja told the FBI that Chen did travel to China with the MacBook laptop. Also, Speartip advised that it discovered the TCC MacBook contained GPS locations in China. Speartip discovered this information by using Meraki Systems Manager, which is a highly reliable software application that facilitates the ability to manage a MacBook's various systems and includes the ability to

recover GPS location information. Speartip's analysis of the MacBook's GPS locations determined the following:

- a. The MacBook was in Rolla, Missouri on April 8, 2016.
- b. The MacBook was in Wuhan, China (location of CNS) from May 4, 2016 to May 5, 2016.
- c. The MacBook was in Shenzhen, China on May 7, 2016.
- d. The MacBook was in Beijing, China (location of Sinochem) on May 8, 2016.
- e. The MacBook was in Taipei, Taiwan (location of Chen's father and two hours away from Wuhan, China) from May 11, 2016 to May 14, 2016.
- f. The MacBook was in St. Louis, Missouri on May 16, 2016.

Results of Analytical Research Regarding Zhang, Zhou and Sinochem

40. FBI St. Louis Division personnel learned the People's Republic of China officially launched the State Key Laboratory of Crop Breeding Technology Innovation (hereinafter referred to as "Key Laboratory") on April 14, 2016. The laboratory aims to develop, integrate and apply crop breeding technology on worldwide agricultural plants by organically combining the latest research results in genomics and molecular biology with conventional breeding techniques in order to continuously launch new green crops with independent intellectual property rights. Zhou was named the laboratory's director, and Zhang was named the director of the laboratory's academic committee. Zhou was also an expert with China's Thousand Talents Program, which per its website www.1000plan.org/en/, seeks to recruit individuals under the age of 55 who are willing to work in China on a full-time basis with full professorships or the equivalent in prestigious foreign universities and research and development institutes.

41. Sinochem is a key state-owned enterprise based in Beijing, China. Core businesses owned by Sinochem span energy production, agriculture, chemical production, real estate and financial services. Sinochem owns CNS, which established the Wuhan Center for Life Science and Biotechnology-the biggest domestic proprietary research and development base in the industry in China. Sinochem was also chosen to run the Key Laboratory under the Ministry of Agriculture for Genetic Breeding of Crops like corn and rice.

42. Based on the above, your affiant concludes that CNS, the LSC, the Key Laboratory and the Key Laboratory under the Ministry of Agriculture for Genetic Breeding of Crops are directly owned and/or operated by Sinochem, an entity of the People's Republic of China.

Results of Forensic Digital, Financial Analysis and Document Review Thus Far

43. FBI St. Louis Division's CART, comprised of the forensic examiners who imaged digital evidence seized during the search of Chen's residence, determined the following via its analysis of the images:

- a. On May 30, 2016, a Chrome cleaner software was run to remove all information from the Chrome Browser on the TCC MacBook, to include all references to Google documents. Open source information indicates Chrome cleaners are used to clean browsers and remove cache and historical records.
- b. On May 30, 2016, the Chrome remote desktop application was removed from the TCC MacBook Pro. Open source information indicates this application allows someone to access other computers or to allow another user to access a computer securely over the internet.
- c. From May 29, 2016 to June 1, 2016, the Clean My Mac program was run each day on the TCC MacBook. Open source information indicates this program

allows a user to scan a MacBook's files, advises what can be removed and removes the selected files.

- d. On May 25, 2016, an iPhone cleaner program was removed from the TCC MacBook. Open source information indicates this program allows a user to sweep an iPhone for needless files and subsequently eliminate caches and other files for the purpose of freeing up memory and other storage space.
- e. On June 1, 2016, the Disk Drill program was run on the TCC MacBook. Open source information indicates this program allows a user to scan and recover data from virtually any storage device, including a MacBook hard-drive and external hard-drive.
- f. On an unknown date, a Diskcartography program was run on the TCC MacBook. Open source information indicates this program is used to scan and analyze disks and folders for the purpose of cleaning and freeing up space.
- g. On an unknown date, an Easeus Mac data recovery program was run on the TCC MacBook. Open source information indicates this program is used to recover deleted, formatted, inaccessible or lost data from Mac notebooks, desktops, digital devices or storage media.
- h. On May 25, 2016, May 27, 2016 and May 30, 2016, Eraserscanner was run on the TCC MacBook. FBI St. Louis Division's CART advised this application is a subcomponent of the Disk Drill Program. Erasescanner looks for different types of files where digital evidence can be found and attempts to delete these files.

- i. From May 25, 2016 thru May 30, 2016, System Cache Scanner, which CART advised is used to look for temporary files in a computer's cache for subsequent deletion, was run on the TCC MacBook.

44. Per CART, the presence of the above applications is consistent with an individual who is actively attempting to remove evidence pertaining to suspicious behavior. Normally speaking, a lay person does not install or look for temporary files or attempt to remove records thereof.

45. A Grand Jury Subpoena served on Google, Inc. produced the following information regarding target email accounts ikhoja@gmail.com and diceros.chen@gmail.com:

- a. On June 17, 2004, ikhoja@gmail.com was created with subscriber name Irma Khoja. It had a recovery email address of diceros.chen@gmail.com and nickname of "Irma" associated with it. Services include Android, Android Market, Fusion Tables, Gmail, Google Alerts, Google Bookmarks, Google Books, Google Calendar, Google Chrome Sync, Google Code, Google Dashboard, Google Docs, Google Drive, Google Groups, Google Hangouts, Google Help, Google Maps Engine, Google Moderator, Google My Maps, Google Payments, Google Photos, Google Play Music, Google Reader, Google Services, Google Voice, Google Webmaster Tools, Location History, Lock SafeSearch, Tasks In Tingle, YouTube and iGoogle.
- b. On June 22, 2004, diceros.chen@gmail.com was created with subscriber name J.R. Chen. It had a recovery email address of chenjiunnren@hotmail.com associated with it. Services included with this email account include Android, Contacts, Gmail, Google alerts, Google Analytics, Google Calendar, Google Chrome Sync, Google Docs, Google Drive, Google Groups, Google Hangouts,

Google Maps, Google maps Engine, Google Moderator, Google My Maps, Google News, Google Notebook, Google Payments, Google Photos, Google Play, Google Reader, Google Services, Google Subscribed Links, Google Voice, Google Wave, Google+, Knowledge Search, YouTube, iGoogle and Orkut.

- c. Based on CART's forensic analysis to date, communications pertaining to both of these email accounts were found on Khoja's MacBook.

46. Through investigation, FBI St. Louis Division has determined the following:

- a. Chen's diceros.chen@gmail.com email account was increasingly used between January 26, 2016, and June 29, 2016, with the bulk of the usage taking place between April 29, 2016, and June 29, 2016.
- b. Khoja's ikhoja@gmail.com email account was used fairly consistently between January 22, 2016, and June 29, 2016, specifically with increased frequency closer to June 29, 2016.
- c. As recently as August 25, 2016, Chen was using his diceros.chen@gmail.com email account. On August 25, 2016, Chen sent an email from his diceros.chen@gmail.com email account to Investor's Title Company. The email was regarding the sale of his 6345 Bancroft Avenue, St. Louis, Missouri, residence and indicates that Chen continues to use the email account while in China.

47. Information received from Google, Inc. indicates that Chen's email account was used on April 30, 2016; May 2, 2016; May 3, 2016; May 4, 2016; and May 5, 2016. These dates are right before Chen went to China for the job interview and right around the time Chen was physically in Wuhan, China. Wuhan, China is the location of Sinochem/CNS. Khoja's email account was used on May 2,

2016; May 3, 2016; May 5, 2016, and May 14, 2016. These dates are before, during, and after their trip to China. It was during this trip to China for the job interview that Chen's TCC MacBook Pro laptop was used and Chen's passwords accessed TCC's Google Drive account. Due to the email correspondence happening before, during and after Chen and Khoja's May trip to China, probable cause exists to conclude these accounts contain evidence, instrumentalities, contraband or fruits of violations of Title 18, United States Code, Section 1030(a)(2)(C) and Section 1832.

48. FBI St. Louis Division's CART reviewed the information obtained from Google and determined diceros.chen@gmail.com was accessed on May 2, 2016 via Simple Link VPN and Choopa VPN and, then again, from May 3, 2016 thru May 5, 2016 via Simple Link VPN. FBI St. Louis Division's CART also determined ikhoya@gmail.com was accessed on May 14, 2016 via Hinet VPN, which is a Taiwanese service.

49. CART also advised that the aforementioned Kingston thumb-drive was inserted into four separate computers. The three known computers it was inserted into are: the MacBook, the ThinkPad Lenovo T440 and a laptop that belonged to one of Chen's neighbors in St. Louis. The Kingston thumb-drive is encrypted. The FBI is currently attempting to break the encryption to be able to review the contents of the thumb-drive.

50. Chen used the neighbor's laptop on June 9, 2016, shortly before his interview with Monsanto personnel at Starbucks. With the consent of the owner of the laptop, CART forensically imaged the neighbor's laptop and subsequently found a list of Chinese sentences that upon initial review appear to relate to agriculture. St. Louis Division is awaiting final translation of these sentences and believes the neighbor does not speak Chinese.

51. Lastly, CART discovered that one of Monsanto's trade secret documents was uploaded into a Google Drive account on an unknown date and that another of Monsanto's trade secret documents

was uploaded into an online data storage facility that facilitates the sharing and amending of information on an unknown date. This facility was formerly known as Wireleaf, but is now known as Overleaf.

Monsanto advised that neither the former upload, which was identified via web-link

<https://drive.google.com/file/d/0B1MzQ-eiEzglOHoycWZKdnNjaFk/view?usp=sharing>, nor the latter upload, which was identified via web-link <https://www.writelatex.com/1575914xtxnjbj#/3922229>, were authorized.

52. Lastly, Monsanto advised that neither it nor TCC owned the aforementioned Google Drive account. Because of this, Monsanto believes this account is a personal Google Drive account. The St. Louis Division of the FBI is attempting to determine subscriber information regarding these accounts.

Financial Analysis

53. Investigators have reviewed transaction histories for Chen and Kohja's bank accounts. On May 16, 2016, Chen deposited \$9,400.00 in cash into his Bank of America checking account XXXX-XXXX-9336 (Checking Account). This deposit was made one day after Chen returned from his job interview in China with Sinochem. The sum of \$9,400.00 is approximately \$600.01 less than the amount that would have required Chen to file a Currency and Monetary Instruments Report (CMIR) had he entered into the country with that sum of money. It is also \$600.01 less than the amount of money that would have required Bank of America to file a Currency Transaction Report (CTR) had Chen deposited such a sum into his bank account. A large cash deposit is also out of character for Chen when compared with his prior banking history. No other similarly large deposits of cash have been observed during the period January 29, 2016 to August 24, 2016.

Chen's Unexpected Departure for China and Sale of His Home

54. Prior to Friday, August 20, 2016, attorneys from Husch have been engaged in continuous discussions with Richard Sindel, counsel for Chen, regarding Chen's mishandling of Monsanto's trade secrets. Those discussions have included attempts by attorneys from Husch to obtain Chen's voluntary cooperation in gaining access to certain devices formerly in Chen's possession. On Friday, August 19, 2016, Husch requested that Mr. Sindel disclose the password for one such portable storage device to assist in recovering data from that device. Mr. Sindel reported that Chen claimed not to recall the password. Mr. Sindel was then asked to provide the answers to certain security questions which could be used to reset the password. The answers provided by Chen, through Mr. Sindel, were not successful in unlocking the device, and, as of the date of this writing, attorneys from Husch have been unsuccessful in gaining access to the encrypted data on the device.

55. Also on August 19, 2016, Husch questioned Mr. Sindel about Chen. Chen's attorney advised that Chen had not accepted any job nor had any future travel plans.

56. At an unknown time on August 19, 2016, Chen and Khoja each signed a separate Durable Power of Attorney, which appointed Richard H. Sindel as their Attorney In Fact to manage financial, real estate, and other affairs.

57. That evening, on August 19, 2016, Chen bought three one-way airline tickets to Shanghai, China for himself, his wife, and his daughter, with a departure date for the very next evening. Chen did not purchase return travel tickets.

58. At 11:30 a.m. on Saturday, August 20, 2016, Chen and his family departed St. Louis Lambert International Airport for Shanghai, China by way of Detroit Metropolitan Airport. After arriving in Shanghai, Chen and his family departed for Wuhan, China on August 21, 2016, at 9:05 p.m. local time. Wuhan, China is where the CNS is located. The FBI believes that Chen is currently in Wuhan, China.

59. Chen informed Customs and Border Patrol personnel (CBP) that he ultimately planned to travel to Taipei, Taiwan. However, Chen's travel itinerary does not reflect this. CBP informed Chen that he needed to return to the United States within six months because failure to do so would violate the terms of his legal permanent resident alien status. Chen, in response to CBP's advisory, stated he would return from Taipei in approximately two months.

60. On Monday, August 22, 2016, Chen sold his family's home, located at 6345 Bancroft, St. Louis, MO 63109 to an individual with the initials C.C. (the "Buyer"). Chen and Khoja were scheduled to appear at Investors Title Company to close on the sale. Instead, to the surprise of Investors Title Company, Mr. Sindel appeared as their attorney in fact and signed documents on their behalf to close on the sale of their residence.

61. In exchange, Chen and his wife received the purchase price of \$193,400.00, which funds were tendered by the Buyer to Investors Title Company, which issued a U.S. bank check #387143 to Jiunn-Ren Chen and Irma Khoja in the total amount of \$111,516.68.

62. On August 25, 2016, a Federal Grand Jury Subpoena was served on Mr. Sindel, who confirmed that he was in possession of check #387143 in the amount of \$111,516.68 payable to Chen and Khoja and it had not been deposited. The subpoena requires Mr. Sindel to turn over the check to the U.S. Government by August 31, 2016. In a conversation with Assistant U.S. Attorneys Richard E. Finneran and Colleen Lang that same day, Mr. Sindel confirmed that in the meantime he would hold the check and would not deposit it.

63. On August 25, 2016, Chen emailed Investors Title from target email account dicerros.chen@gmail.com regarding the check.

Filter Team Procedures

64. Chen's wife, Irma Khoja, is a licensed attorney in the state of Florida. Due to her status as a licensed attorney and the fact that there may be email correspondence between Chen's attorney and Chen, filter team procedures are in place to search the email accounts of akhoja@gmail.com and disceros.chen@gmail.com. The filter team will review the information Google sends the FBI on these email accounts. The results from Google will be copied by a member of the filter team or its designated agents (not part of or related to the case investigative or prosecution team). Filter team agents will then review the copies to locate files, data, records, or other materials related to the scope of the items seized under the warrants ("relevant materials"). The filter team agents will electronically search, copy, or print out relevant material and forward the relevant materials to the filter team AUSA. Filter team agents will also forward to the filter team AUSA (who is not part of the investigation) all materials that the agents are uncertain whether they fall within the scope of the warrant. The filter team AUSA will determine whether such materials fall within the scope of the warrant. The filter team AUSA or agent shall not disclose the contents of any potentially privileged materials to any investigative agent or prosecutor.

CONCLUSION

65. Based on the foregoing, there is probable cause to believe that Chen violated Title 18, United States Code, Sections 1030(a)(2)(C) (Fraud and Related Activity in Connection with Computers) and 1832 (Theft of Trade Secrets) when he intentionally accessed a protected computer without authorization and/or exceeded authorized access and subsequently obtained trade secret information from that computer. There is also probable cause to believe that evidence of these crimes; contraband; fruits of these crimes; and/or instrumentalities of these crimes further described in Attachment B currently exist in these email accounts. Your affiant therefore requests the Court issue a search warrant

authorizing a search of the aforementioned accounts and authorizing the seizure of the items described in Attachment B.

66. On June 15, 2016, Federal Bureau of Investigation personnel sent a preservation letter to Google, Inc., specifically to preserve all records that pertain to email accounts ikhoja@gmail.com and dicerros.chen@gmail.com. In general, an email that is sent to a Google, Inc. is stored in the subscriber's "mail box" on Google, Inc.'s servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google, Inc.'s servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google, Inc.'s servers for a certain period of time.

67. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, Inc., which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

68. I further request the Court order all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Gmail email accounts ikhoja@gmail.com and disceros.chen@gmail.com that are stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountainview, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on June 15, 2016, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)(2)(C) (Fraud and Related Activity in Connection with Computers) and 1832 (Theft of Trade Secrets), those violations involving Jiunn Ren Chen and occurring from April 2016 through the present, including, for each account or identifier listed in Attachment A, information pertaining to the following matters:

- (a) Monsanto's proprietary and/or trade secret information; Chen's discussion thereof with representatives of foreign companies that specialize in agricultural matters; and the transfer thereof to representatives of foreign companies that specialize in agricultural matters;
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation; and
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).